Self guardianship at automated teller machines

Matthew P J Ashby, School of Social Sciences, Nottingham Trent University
Adam Thorpe, Design Against Crime Research Centre, University of the Arts London

This is a post-peer-review, pre-copyedit version of an article published in Crime Prevention and Community Safety. The definitive publisher-authenticated version is available online at: http://dx.doi.org/10.1057/s41300-016-0010-3

Abstract

Automated teller machines (ATMs) are central to the functioning of developed economies, but by their very nature operate without human supervision, making them vulnerable to criminal abuse. This study sought to understand how customers protect themselves from theft while using ATMs. Observations of and surveys with ATM customers were used to identify how individuals protect themselves from theft of cash, card or personal details while using an ATM. The most common self-guardianship measure was to use only ATMs believed to be safe. The majority of customers did not cover the ATM keypad while entering their personal identification number (PIN), despite long-running publicity campaigns encouraging this behaviour. This suggests that self guardianship is important at ATMs, but many customers fail to take even basic measures to protect themselves, their money and their bank details from theft. Banks and crime-prevention practitioners should do more to facilitate and encourage self guardianship at ATMs.

Keywords. Automated teller machine, situational crime prevention, self guardianship

Introduction

Automated teller machines (ATMs) were developed by banks in several countries in the late 1960s, allowing banks to reduce costs and giving customers access to a limited subset of banking services at any time of day (Bátiz-Lazo and Reid, 2011: 32). ATMs have become common, with more than two million in use worldwide in 2010 (PCISSC, 2013: 8). In the United Kingdom (UK) 92% of adults used an ATM in 2009, performing a total of 2.9 billion transactions that provided 72% of all cash to individuals (Mott and Townsend, 2010: 2). ATMs are attractive to thieves because they provide a ready source of money at a time when the use of cash in other areas of society is declining. This study examined how people protect themselves while using an ATM, which is important because the "automated" nature of ATM transactions usually means there are no bank staff to protect customers.

The routine-activities approach to studying crime (Cohen and Felson, 1979) understands criminal events in terms of opportunities, said to occur when a motivated offender and a suitable target converge in time and space. The likelihood of an opportunity resulting in a crime occurring depends upon the presence or absence of different actors who influence each element of the event. Offender *handlers* (Felson, 1986) influence offender motivation, while place *managers* (Eck, 1995: 70) influence the likelihood of an offender and target meeting. The present study is concerned with the *guardian*, a third actor who influences the suitability of a target to attack. Individuals who provide guardianship are usually not specifically employed or trained to prevent crime, they are simply able to do so because of circumstance. The presence of passers-by can provide effective guardianship (Felson and Boba, 2010: 28), but only if members of the community look out for one another. Newman (1972: 79) argued that community members are more likely to act as guardians when they have "proprietary feelings" towards the target of a crime. This may well be the case in residential areas where neighbours know, and feel a responsibility to protect, one another – Reynald (2009) found that levels of guardianship were higher in areas with more social interaction between neighbours. ATMs are situated in such areas, but also in town centres, out-of-town shopping areas and other places where most people are not local, or are only occasional visitors. In such places, the ATM customer themselves may be the only person able to protect themselves.

There has been some disagreement in the literature about whether people can be guardians of themselves or their own property (Reynald, 2014: 2488) – what Sampson et al (2009: 46) referred to as "self guardianship". Hollis et al. (2013: 74) argued that only third parties can be guardians, and that self-protection should instead be referred to as target hardening. This term, however, has previously been used to refer specifically to strengthening the physical security of inanimate objects (see, for example Mayhew, 1984; Clarke, 1997), which is only one type of guardianship activity. Sampson et al. (2009: 44), conversely, argued that "much guardianship is self-guardianship – people taking action to protect themselves". This argument conceives of guardians as people who protect targets, whatever other roles they may have in a particular criminal act. The human elements described in the routine-activities model – offenders, targets, handlers, guardians, managers etc – are roles, rather than necessarily being separate actors. Eck and Madensen (2015) described how a single actor can fulfil multiple roles within the model. There appears to be no particular reason why a person can simultaneously be (for example) both a place manager and an offender handler but cannot simultaneously be a target and a guardian. The concept of self-guardianship appears to becoming increasing accepted in the literature and to be useful for analysis of criminal events (see, for example Franklin et al, 2012; Giblin, 2008; Reyns et al, 2011), and so will be used in this paper.

The advantages of self guardianship are obvious: if people guard themselves then there will be as many guardians as targets, and each target will have a guardian constantly present. Nevertheless self-guardianship may be ineffective if the guardian is not capable, perhaps because they do not appreciate a particular risk of victimisation, have misunderstood it, or are physically incapable of guarding against an offender.

Understanding the nature of self guardianship by potential victims is important for two reasons. Firstly, many crime-prevention activities (such as publicity campaigns and self-defence classes) are based on shaping or encouraging self guardianship. Such activities are more likely to be successful if those implementing them understand the existing level of baseline self guardianship. Secondly, other forms of crime prevention may be more likely to be effective if they take into account the nature of self-guardianship carried out by potential victims.

ATMs are one of many innovations that have increased the usability of a product or service while also presenting new security challenges (Braz et al, 2007) – the "troublesome trade-off" between promoting use and avoiding abuse (Ekblom, 2005: 217). In the case of ATMs, it is necessary for the bank to make access as easy as possible for customers while simultaneously preventing access by offenders.

The frequency of ATM crime is not known, because in the UK police record offences according to the law broken rather than environmental characteristics. Attacks on ATM customers can be divided into two types: those that target the interface between the customer and the machine, and those that target the customer directly[1]. Human–machine interface attacks focus on obtaining details of a customer's bank card and personal identification number (PIN). Card details can be obtained by fitting a device to the card slot on the ATM, allowing the customer to insert a card but preventing the machine from returning it (Sakharova and Khan, 2011: 17). These *card trap* attacks are effective, but only one card can be captured before the offender must return to the machine (ENISA, 2009: 16). Since the customer's PIN is not recorded anywhere on a bank card (ISO, 2011: 13), card-trap offenders wishing to obtain the PIN must do so separately. One alternative is to instead place a *cash trap* over the slot through which the ATM dispenses cash, so that the customer cannot retrieve the cash but the offender can.

A more efficient method is to fit a *card skimmer* over the ATM card slot. A skimmer can read the card number from the magnetic strip on the reverse of a bank card as the customer inserts the card into the machine (Masters and Turner, 2007). Skimmers are camouflaged to encourage customers to believe that they are a legitimate part of the ATM, and (because they allow the machine to return the customer's card) can typically collect details of many cards without detection (ENISA, 2009: 14). Some skimmers include a miniature camera that records video of the customer typing their PIN, or a false keypad fitted over the genuine keys. If the offender does not have access to a camera or replacement keypad, it will be necessary for them to obtain a customer's PIN by observing the customer typing it, typically by loitering close to the machine and watching the customer, known as *shoulder surfing* (ENISA, 2009: 17).

Once an offender has obtained a card number, he or she can clone the card. If the offender also knows the relevant PIN, the card can be used at an ATM to withdraw

cash. Even without knowing the PIN, the offender can use the card number in transactions on the internet or over the telephone, known as *card not present* fraud (Kosse, 2013: 78). Offenders involved in stealing details from many cards can also sell those details in bulk to organised crime groups via specialist online forums (Europol, 2012: 10).

In addition to these attacks against the customer's card details, thieves can target cash – or the bank card itself – once a customer has removed it from the ATM. In many cases this is done by *pick-pocketing*, made easier for offenders because they can observe where the customer puts the money after using the ATM. Such offenders may seek to distract the customer, for example by spilling a drink onto their clothing or by one offender bumping into the customer while a second steals cash or card (Johnson et al, 2010: 7). An alternative to pickpocketing is to use violence or threats to *rob* the customer. Such offences are not unique to ATMs, but robbing ATM customers may be attractive to thieves because the presence of the ATM ensures a steady flow of potential targets who are known to have cash in their possession (Holt and Spencer, 2005: 16).

Although thefts from customers at ATMs have been a subject of previous research (e.g. Guerette and Clarke, 2003), little of this has focused on customer behaviour. Kosse (2013) reported on a survey of the perceptions of 1,672 Dutch citizens of the security of different methods of retail payment. Five percent of customers reported that they had previously been a victim of card skimming at an ATM. Ten percent reported feeling that using an ATM was unsafe, more than had the same feelings about using cash (2%), debit cards (4%) or credit cards (6%). Customers who felt ATMs were unsafe were more likely to prefer not using ATMs.

The authors were able to find only one brief conference paper that attempted to answer similar questions to those being asked here. De Luca et al (2010) observed transactions at six ATMs in the Netherlands and Germany, then carried out a survey of 25 customers in Switzerland. They found that 35% of customers made an observable attempt to cover the ATM keypad when entering their PIN, usually by holding their other hand or their wallet over the keypad. The proportion of customers actually covering their PIN was substantially lower than the 19 out of 25 participants who claimed that they always do so. Some participants stated that they normally cover their PIN, but would not do so if accompanied by a friend. Survey participants also

mentioned taking other security measures, such as only using ATMs in buildings or a familiar ATM, although the small sample size precluded extrapolation to the wider population.

The present study was concerned with the theft of cash, bank cards, bank-card numbers or card PINs from customers while they were using an ATM or immediately afterwards. This included dishonest or fraudulent acquisition of a customer's card number, PIN or cash by shoulder surfing, distraction theft, pickpocketing or robbery, or by using a card skimmer, card trap, cash trap, covert camera or false keypad. Within this definition of ATM crime, the study attempted to answer two questions.

1. How do people seek to protect themselves from becoming victims of theft related to their use of an ATM?
2. How do any security measures that customers take differ depending on
    a. the age and gender of the customer,
    b. the environment the customer is in, and
    c. whether or not the customer has previously been a victim of ATM crime?

Methods

This study used observation of ATMs transactions combined with post-observation surveys with a sub-group of customers having conducted those transactions. A total of 2,640 observations were carried out at 22 ATMs at ten sites in Camden and Westminster, two boroughs in central London. The sites selected were hot spots for ATM crime: i.e. those places with the highest number of personal robbery, theft from the person and deception offences recorded by police in the three years before the study began, with these offences being associated with an ATM if the offence address was recorded as being at, near or outside the relevant bank. All the ATMs observed were embedded into the external wall of a bank so as to be accessible to customers on the street – this is by far the most common type of ATM in the UK.

All of the ATMs observed in this study are operated by the same bank, but the machines were not all of the same model or supplied by the same manufacturer. Retail banking in the UK is provided by a small number of large banks that operate across the country, and there are few differences between the customer-facing ATM operations of

the different banks. With a few exceptions, UK bank customers can (and often do) use ATMs operated by any bank without paying a charge, so the authors do not believe the decision to observe ATMs from one bank substantially limits the generality of the results. Both the bank operating the ATMs and the local police were made aware of the observations before they began.

The ten study sites were observed for approximately 30 minutes a day, three days a week (Monday, Tuesday and Friday) for two periods of 8 weeks during the summer of 2012. Every transaction occurring during an observation period was recorded. Since the observations were conducted over several weeks, some customers may have been observed more than once, but there was no way for the observers to identify such cases.

To ensure that time of day, daylight levels and bank opening hours did not influence the results, every site was observed an equal number of times for each 30-minute period between 1100 and 2000. These times were chosen to ensure that there were sufficient transactions to observe. To maximise consistency of observations, observers were briefed before observations began, observations were recorded on a structured recording form and post-observation debriefs were conducted. Observers were stationed at pre-set points approximately ten metres from the nearest ATM (or group of ATMs), close enough that they could observe customers but far enough away that they were unlikely to influence customer behaviour. Observers were casually dressed and there were no incidents during the observations that indicated that customers were influenced by, or even aware of, the presence of observers. Observation locations were selected so that observers could gather data – including being able to see whether or not the customer covered their PIN – while not being close enough to be able to read the text on the ATM screen or see the PIN itself. PIN covering was recorded as it was seen by the observer, but it is possible that (for example) even though the observer believed the PIN to be covered, a person in another position could have been able to see the PIN. Observers were required to remain stationary so as not to influence customer behaviour and to ensure consistency of observations, so it was not possible for observers to make observations from multiple angles for each customer.

For each ATM transaction, the observer recorded data about the customer and the environment surrounding them. The customer's age was estimated by the observer[2]. The emphasis placed on ensuring that the presence of observers did not influence the

behaviour of customers meant that the information that observers could record was limited. For example, it was not possible to record whether the observer checked for suspicious devices on the machine prior to using it, because many such checks would be done simply by looking at the machine so there would be no physical behaviour for the observer to see.

During the final week of each eight-week observation period, observations were combined with surveys. During this period, after a customer had used an ATM they were approached by the observer and asked to complete a short survey (see Appendix A). A total of 276 customers agreed to participate in the survey, a response rate of 65% of those observed during the survey period. By approaching customers only after their ATM usage had been recorded by the observer, it was possible to ensure that observed behaviour was not influenced by the survey questions.

An exploratory approach to analysis was used due to the nature of the research questions. Cramer's V (Cramer, 1946) was calculated for chi-squared (χ^2) tests to quantify the association between variables. Values of V vary between zero – meaning no association between the two variables – and one – meaning complete association. Multivariate analysis was done using binary logistic regression. Note that because of multiple comparisons, readers should exercise caution in interpreting results that only just reach statistical significance.

Results

A total of 2,640 customers were observed using an ATM. At one site an observer witnessed a customer discovering – and bank staff subsequently removing – a card skimmer from an ATM. At another site, bank staff challenged an observer whom they had noticed loitering close to the ATMs. However, none of the customers who were observed challenged the observers directly.

[TABLE 1 ABOUT HERE]

The third column of Table 1 shows the distribution of participants for each variable recorded by the observers, divided into variables relating to the customer, their behaviour and the environment around them. Forty-seven percent of customers

attempted to cover the ATM keypad when entering their PIN, of which 52% (24% of all customers) covered the keypad effectively so that the observer could not see the keypad. The remaining 48% of customers who attempted to cover the keypad (23% of all customers) did so ineffectively, such that the keypad was still visible to the observer and the PIN would still have been visible to the observer should they have been standing closer to the customer.

The fourth column of Table 1 shows the proportion of customers attempting to cover their PIN according to each recorded variable. Table 2 shows the results of binary logistic regressions run to determine which individual and situational variables predicted whether or not a customer would attempt to cover their PIN. Further models were run with the location of the observation added as an additional predictor, but this did not lead to any significant change in the results.

[TABLE 2 ABOUT HERE]

The PIN-covering model was significant ($\chi^2(11) = 32.06$, $p < 0.01$) but weak (Nagelkerke $R^2 = 0.02$). Only two individual predictors were statistically significant: both the customer being aged 25–35 years (compared with being under 25 years) and the presence of people passing by were associated with fewer people attempting to cover their PIN.

A total of 276 ATM customers took part in the survey, a mean of 28 per site. Two thirds of participants were male and all participants were aged under 50 years. Approximately one third of participants fell into each of three age groups: 24 years and under, 25–34 years and 35–49 years. Eight percent of participants had previously been a victim of ATM crime.

Ninety percent of participants said that they were conscious of security when using ATMs. A logistic regression using age, gender and location of participants, and whether or not they had previously been a victim of ATM crime, showed that none of these variables were significant predictors of whether a person would be conscious of ATM security or not ($\chi^2(12) = 11.06$, $p = 0.52$, $R^2 = 0.09$, co-efficient values available from authors on request).

[TABLE 3 ABOUT HERE]

Participants who said they were conscious of security were asked “what security issues are you conscious of?" with participants' responses coded for analysis and the results shown in the second column of Table 3. To determine whether the security issues of concern to participants varied according to their age, gender or location, a logistic regression was run with those variables as predictors. Since participants could report concern about more than one security issue, one regression was run for each issue. Table 3 shows that in no case were age, gender, location or previous victimisation significant predictors of whether or not a person would be concerned about a particular security issue.

[TABLE 4 ABOUT HERE]

Participants were then asked “How does concern about ATM security influence your behaviour when using an ATM?" This was an open question with participants' answers coded as shown in Table 4. Almost nine out of ten participants claimed that they took some action, regardless of their gender ($\chi^2(1) = 0.21$, $p = 0.65$, $V = 0.03$) or age ($\chi^2(2) = 2.68$, $p = 0.26$, $V = 0.10$). There was no relationship between whether a person had previously been a victim of ATM crime and whether or not they claimed to take security measures ($\chi^2(1) = 0.26$, $p = 0.61$, $V = 0.03$). This may be due to the low number of victims in the survey and the high number of those claiming to take at least one security measure. Being conscious of ATM security was strongly associated with participants claiming to take action against perceived threats ($\chi^2(2) = 169.50$, $p < 0.001$, $V = 0.78$): 96% of people who said they were conscious of ATM security took steps to keep themselves safe while using an ATM, compared to 14% of people who were not conscious of security threats.

The measures that participants described can be grouped into those concerning the choice of which ATM to use and those actions concerning how the participant uses that ATM. The most common measure in the first group, mentioned unprompted by over one quarter of participants, was to only use certain ATMs. To probe the factors influencing choice of ATM, participants were asked to choose from a list of potential

factors, as shown in Table 5. It seems that the appearance and location of an ATM are particularly important in customers' decisions. Also shown in Table 5 are the results of binary logistic regression models showing that in no case were the age, gender, location or previous-victimisation status of the participant a significant predictor of whether participants considered a particular factor or not.

[TABLE 5 ABOUT HERE]

The most commonly stated security measures taken by participants *after* they had chosen an ATM were covering the keypad while entering their PIN (mentioned by 19% of participants), checking the machine for suspicious devices (mentioned by 18%) and checking the surrounding area (for example for suspicious people, mentioned by 12% of participants).

After being asked what security measures they took without prompting, participants were asked whether or not they took the specific security measures shown in Table 6. It can be seen that the number of participants reporting taking a particular security measure in answer to the closed question was substantially higher than the number of participants who mentioned the same measure in their answers to the open question (shown in Table 4).

[TABLE 6 ABOUT HERE]

The final question asked “have you ever wanted to request privacy while using an ATM", to which 85% of respondents answered `yes'. Of those participants who wanted to request privacy, only 39% reported that they felt able to do so, with the remainder having wanted to ask for privacy but not having asked for it. Further logistic regressions showed that neither the proportion of people wanting privacy nor the proportion asking for it varied by age, gender, location or previous victimisation (wanting privacy: $\chi^2(12) = 11.58$, $p = 0.48$, $R^2 = 0.08$; asked for privacy: $\chi^2(12) = 13.88$, $p = 0.31$, $R^2 = 0.09$).

Participants were surveyed after they had been observed using an ATM so that it was possible to compare their behaviour with their answers during the survey. Of the 90% of observed participants who claimed that they cover the ATM keypad when entering their

PIN, 74% were observed to attempt to do so: 53% actually covered the keypad, obscuring their PIN details, while a further 21% made an ineffective attempt to cover the keypad and 26% made no apparent attempt to do so.

Discussion

The survey conducted for the present study show that almost all ATM customers are concerned about security while using an ATM, regardless of their age, their gender or whether they have previously been a victim of ATM crime. Although taking preventative action appears to be dependent upon a customer being concerned about security, the vast majority of customers expressed such concern. Customers appear to be aware of a broad range of security threats, with participants mentioning all of the main types of customer-focused ATM crime discussed above. Concern about ATM security appears to be a necessary, but not sufficient, condition for taking steps to reduce the likelihood of victimisation.

Almost all participants who were aware of ATM security threats claimed to take some action, again regardless of age, gender or previous victimisation. The most common action taken was to use only certain ATMs, particularly those believed to be safe due to their surroundings and or conditions. This finding may be of interest to banks because in the UK a bank receives a fee whenever one of their ATMs is used by a customer of another bank, and so banks have an incentive to make their own ATMs as attractive as possible. Banks wishing to maximise ATM usage may benefit from publicising the security features of their own ATMs, particularly in inner cities where there are many bank branches and customers can easily choose between ATMs operated by different banks.

Participants' stated preference for ATMs in areas that appear to be safe and familiar suggests that customers seek out environments where natural surveillance, either by passers-by or by the customer themselves, is most likely to be effective. Given that ATMs are often situated in non-residential areas, customers may be searching for a site that replicates, to the extent possible, the natural surveillance that protects them when they are in their own neighbourhood.

While almost all participants stated that concern about ATM security caused them to take action to protect themselves, it is notable that most customers did not cover their

PIN. A secure PIN is the primary means by which banks ensure that a person using an ATM is authorised to have access to a particular bank account, so banks in many countries have for several years run campaigns encouraging customers to cover their PIN when using an ATM. All of the ATMs observed in the present study featured an on-screen message reminding customers to cover their PIN. Despite this timely reminder, most customers did not attempt to cover their PIN and almost half of those who did were ineffective in hiding the PIN from observers.

A review by Barthe (2006) found that crime-prevention advice was more likely to be effective at reducing crime if it was specific to a particular type of crime and was provided so that it was timely and relevant to potential victims. In this respect, the banks appear to be doing everything correctly: the advice given is specific to ATM crime, and it is both timely and relevant. The high proportion of customers not covering their PIN may therefore indicate either that the content of the advice given is ineffective, or that there is a general limitation on the effectiveness of victim-focused crime-prevention publicity in this context. Further research to test the impact of varying the content of on-screen PIN-covering reminders, or development and testing of other measures to do so, may therefore be beneficial in helping banks to increase the proportion of customers covering their PIN.

The regression models run to determine whether individual and environmental variables predicted whether a customer would cover their PIN suggested that customers either use these protective measures or they do not, largely regardless of circumstance. This may be a positive result for crime-prevention practitioners: it suggests that if a customer can be convinced to either cover their PIN, they may begin to do so habitually. The notable exception to the apparent lack of influence of environmental variables was that people were less likely to cover their PIN if there were people passing by. This may suggest that when there are other potential guardians present, people feel that there is less need to guard themselves.

It may be possible to change the design of ATMs to encourage self-guardianship. The concept of "affordances" (Norman, 1999) – "what [the design of] an object `invites' the actor to do" (Farrell and Pease, 2008: 119) – may be useful in designing an ATM that encourages users to behave in a way that promotes their security. For example, the physical design of the ATM keypad could be adapted to `invite' users to cover their

PIN. Doing so may be more successful than simply placing a notice on the ATM encouraging PIN covering (for further discussion of affordances and crime, see Pease, 2006).

Perhaps the most fruitful potential SCP technique for ATM security concerns the siting of ATMs and the design of the surrounding environment. The results of the present study show that customers prefer ATMs that are in secure and/or busy areas, and that appear clean, new or `safe'. Many ATMs are sited in places in which the ATM is peripheral to the main purpose of the facility, for example where they are provided in public transport stations or shopping centres. The secondary nature of the ATM function (from the point of view of the facility owner) is often reflected in placement of ATMs away from the busiest areas, possibly because space in busy areas is at a premium and the owner chooses to use it for their core business. This leads to ATMs being placed in hallways, adjacent to public toilets, in car parks and in other out-of-the-way areas. Placing ATMs in central positions may facilitate customers' self-guardianship and encourage more people to use such machines. Increased ATM use would provide banks with additional usage fees, which may offset any additional money banks would be required to pay to secure premium space (although the economics may vary from case to case).

The data collection methods used in the present study were designed to make the results applicable to customers' use of ATMs in a busy inner-city environment. All of the ATMs observed were on busy streets surrounded primarily by shops and offices. This is a common environment in which ATMs are found in the UK, but the observation results may not be generalisable to the behaviour of customers using ATMs in different environments, such as outside rural bank branches or out-of-town shopping centres.

Survey respondents were selected from customers using the ATMs under observation. As such the results may not necessarily be reflective of the wider inner-city population or of people in other environments. This is important because choosing ATM customers for survey will mean that the results will not capture responses from any potential customers who are so concerned about security that they do not use ATMs at all. All observations and surveys were conducted between 1100 and 2000 hours, so the results may not be generalisable to other times of day. Research covering rural

locations or other times of day would have been problematic, because the lower rate of ATM use would have meant longer observations at greater cost, and would have made it difficult for the observers to have remained unnoticed.

There were substantial differences between the proportion of survey participants who claimed to take security measures (particularly PIN covering) and the proportion actually observed to have done so. This was not unexpected, since the long-standing advice from banks to cover PINs may have led some participants to claim they took certain measures because they believe that doing so is expected of them, rather than because they actually take such action (for a discussion of social-desirability bias in criminological research, see Sutton and Farrall, 2005).

The results of this study suggest several potentially useful avenues for future research. The present study has provided evidence that many ATM customers do not cover their PINs – it would be useful for crime-prevention practitioners to know why this is. A simple survey would be likely to suffer from the social-desirability bias mentioned above, but this problem could be overcome using a post-observation survey with questions tailored to whether the participant had been seen to cover their PIN or not. The results of that research could be used to design measures to encourage PIN covering, which could be evaluated for their effectiveness. It would also be valuable to investigate the interactions between different protective measures. For example, do customers choose not to cover their PIN because they have already selected an ATM they believe to be safe? Such research would require a larger survey sample than was available here. Finally, it may be a useful contribution to the research on guardianship to determine whether the finding that ATM customers were less likely to cover their PIN in the presence of other people might be because they felt that those people provided them with additional guardianship.

The results of the present study indicate that ATM customers are both concerned about becoming a victim of theft and take steps to reduce that risk. The most common step taken is to use only ATMs that are in environments that provide natural surveillance, followed by covering the keypad while entering a PIN. Nevertheless, despite extensive publicity campaigns by banks encouraging various ways in which customers can protect themselves at ATMs, only around half of users take even basic measures such as PIN covering. These results suggest that – in the absence of formal

surveillance or place managers at most ATMs – banks should do more to encourage and facilitate customers to protect themselves.

Acknowledgements

The authors thank the Royal Bank of Scotland Group plc for funding and facilitating this research, as well as staff of the Metropolitan Police Service, the London Borough of Camden and the City of Westminster for their assistance.

Notes

[1] It is also possible to attack the machine directly, or to attack bank staff servicing a machine, but such attacks are outside the scope of the present study.

[2] Ages were subsequently categorised and – for people who were observed and subsequently surveyed – compared with the ages given by participants during the survey. Eighty-three percent of ages estimated by observers were in the same age category as given by the survey respondents.

References

Barthe, E. 2006. *Crime prevention publicity campaigns*. Washington, DC: US Department of Justice.

Bátiz-Lazo, B., and Reid, R. J. K. 2011. "The development of cash-dispensing technology in the UK". *IEEE Annals of the History of Computing*, Vol. 33, No. 3, pp 32–45. doi: 10.1109/MAHC.2010.3

Braz, C., Seffah, A. and M'Raihi, D. 2007. "Designing a trade-off between usability and security: a metrics based-model". In Baranauskas, C., Palanque, P., Abascal, J. and Junqueira Barbosa, S. D. (Eds.), *Human-computer interaction – Interact 2007*, part II (Vol. 4663, pp. 114-126). Berlin: Springer. doi: 10.1007/978-3-540-74800-7_9

Clarke, R. V. 1997. "Introduction". In Clarke, R. V. (Ed.) *Situational Crime Prevention: successful case studies* (pp 1–43). Monsey, NY: Criminal Justice Press.

Cohen, L. E. and Felson, M. 1979. "Social change and crime rate trends: a routine activity approach". *American Sociological Review*, Vol. 44, No. 4, pp 588–608.

Cramér, H. (1946). *Mathematical methods of statistics*. Princeton: Princeton University Press.

Eck, J. E. 1995. "A general model of the geography of illicit retail marketplaces". In Eck, J. E. and Weisburd, D. (Eds.), *Crime and place* (pp. 67–93). Monsey, NY: Criminal Justice Press.

Eck, J. E., and T. D. Madensen. 2015. "Meaningfully and artfully reinterpreting crime for useful science: an essay on the value of building with simple theory". In Andresen, M. A. and Farrell, G. (Eds.) *The Criminal Act: the role and influence of routine activity theory* (pp 5–18). Basingstoke: Palgrave Macmillan.

Ekblom, P. 2005. "Designing products against crime". In Tilley, N. (Ed.), *Handbook of crime prevention and community safety* (pp. 203–244). Cullompton, Devon: Willan.

ENISA. 2009. *ATM crime: overview of the European situation and golden rules on how to avoid it*. Heraklion: European Network and Information Security Agency.

Europol. 2012. *Payment card fraud in the European Union: perspective of law enforcement agencies*. The Hague: Europol.

Farrell, G. and Pease, K. 2008. Repeat victimisation. In Wortley, R. and Mazerolle, L. (Eds.), *Environmental criminology and crime analysis* (pp. 117–135). Cullompton, Devon: Willan.

Felson, M. and Boba. R. 2010. *Crime and everyday life* (4th ed.). Thousand Oaks, CA: Sage. doi: 10.4135/9781483349299

Franklin, C. A., Franklin, T. W., Nobles, M. R. and Kercher, G. A. 2012. "Assessing the Effect of Routine Activity Theory and Self-Control on Property, Personal, and Sexual Assault Victimization". *Criminal Justice and Behavior*, Vol. 29, No. 10, pp 1296–1315.

Giblin, M. J. 2008. "Examining Personal Security and Avoidance Measures in a 12-City Sample". *Journal of Research in Crime and Delinquency*, Vol. 45, No. 4, pp 359–379.

Guerette, R. T. and Clarke, R. V. "Product life cycles and crime: automated teller machines and robbery". *Security Journal*, Vol. 16, No. 1, pp 7–18. doi: 10.1057/palgrave.sj.8340122

Hollis, M. E., M. Felson, and B. C. Welsh. 2013. "The capable guardian in routine activities theory: a theoretical and conceptual reappraisal". *Crime Prevention and Community Safety*, Vol. 15, pp 65–79.

Holt, T. and Spencer, J. 2005. "A little yellow box: the targeting of automatic teller machines as a strategy in reducing street robbery". *Crime Prevention and Community Safety*, Vol. 7, No. 2, 15–28. doi: 10.1057/palgrave.cpcs.8140215

ISO. 2011. *Personal identification number (PIN) management and security – Part 1* (Vol. 1; ISO Standard No. 9564-1:2011). Geneva: International Organization for Standardization.

Johnson, S. D., Bowers, K. J., Gamman, L., Mamerow. L. and Warne, A. 2010. *Theft of customers' personal property in cafés and bars* (No. 60). Washington, DC: US Department of Justice.

Kosse, A. 2013. "The safety of cash and debit cards: a study on the perception and behaviour of Dutch consumers". *International Journal of Central Banking*, Vol. 9, No. 4, pp 77–98.

Masters, G. and Turner, P. 2007. "Forensic data recovery and examination of magnetic swipe card cloning devices". *Digital Investigation*, Vol. 4, pp 16–22. doi: 10.1016/j.diin.2007.06.018

Mayhew, P. 1984. "Target-hardening: how much of an answer?" In Clarke, R. V. (Ed.) *Coping with Burglary: research perspectives on policy*, (pp 29–44). Dordrecht: Springer.

Mott, G. and Townsend, A. 2010. *About the ATM industry* (2nd ed.). unknown: ATM Security Working Group.

Nagelkerke, N. J. D. 1991. "A note on the general definition of the coefficient of determination". *Biometrika*, Vol. 78, No. 3, pp 691–692. doi: 10.2307/ 2337038

Newman, O. 1972. *Defensible space: crime prevention through urban design*. New York: Macmillan.

Norman, D. A. 1999. "Affordance, conventions, and design". *Interactions*, Vol. 6, No. 3, 38–43. doi: 10.1145/301153.301168

PCISSC. 2013. *Information supplement: ATM security guidelines*. Wakefield, MA: Payment Card Industry Security Standards Council. Retrieved from

https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf

Pease, K. 2006. “No through road: closing pathways to crime”. In K. Moss and M. Stephens (Eds.), *Crime reduction and the law* (pp. 50–66). Abingdon: Routledge.

Reyns, B. W., Henson, B. and Fisher, B. S. 2011. “Being pursued online: applying cyberlifestyle-routine activities theory to cyberstalking victimization”. *Criminal Justice and Behaviour*, Vol. 38, No. 11, pp 1149–1169.

Sakharova, I. and Khan, L. 2011. *Payment card fraud: challenges and solutions* (No. 34-11). Dallas: University of Texas at Dallas.

Reynald, D. M. 2009. “Guardianship in action: Developing a new tool for measurement”. *Crime Prevention and Community Safety*, Vol. 11, pp 1–10. doi: 10.1057/cpcs.2008.19

Reynald, D. M. 2014. “Informal guardianship”. In Bruinsma, G. J. N. and D. Weisburd, D. (Eds.), *Encyclopedia of Criminology and Criminal Justice* (pp. 2480–2489). New York: Springer.

Sampson, R., Eck, J. E. and Dunham, J. 2009. “Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure”. *Security Journal*, Vol. 23, No. 1, pp 37–51. doi: 10.1057/sj.2009 .17

Sutton, R. M. and Farrall, S. (2005, March). Gender, socially desirable responding and the fear of crime. *British Journal of Criminology*, Vol. 45, No. 2, pp 212–224. doi: 10.1093/bjc/azh084

Table 1: Customer characteristics and protective behaviours (n=2,640)

		customers (%)	customers attempting to cover pin (%)
all customers	all values	100	47
customer			
apparent age	<25 years	27	52
	25–34 years	37	44
	35–49 years	28	48
	>=50 years	8	45
apparent sex	female	40	48
	male	60	47
customer behaviour			
smoking	yes	12	45
	no	89	47
using mobile phone	yes	5	54
	no	95	47
carrying bag	in hand	27	44
	on shoulder	18	57
	on floor	5	47
	>1 bags	8	48
	no bags	43	45
accompanied	yes	8	53
	no	92	47
environment			
passers by	yes	73	46
	no	27	51
queue at ATM	yes	37	50
	no	63	46
people standing close to	yes	9	45
ATM	no	91	48
another person in position to	yes	2	33

see keypad	no	98	48

Table 2: Predictors of PIN covering

Dependent variables:	PIN covering	
Independent variables	odds ratio	S.E.
aged 25–34 years†	0.67***	0.11
aged 35–49 years†	0.89	0.12
aged 50 years or older†	0.72	0.18
male	0.94	0.09
smoking	0.9	0.14
using mobile phone	1.34	0.2
carrying a bag in their hand	0.83	0.1
accompanied	1.26	0.17
people passing by	0.78*	0.1
queue at ATM	1.13	0
people standing near to ATM	0.96	0.17
other person could see ATM keypad	0.62	0.32
constant	1.36*	0.14

* $p<0.05$ ** $p<0.01$ *** $p<0.001$ †compared to customer under 25 years

Table 3: Relationship between age, gender and location versus concern about security risks

Table shows logistic regression results, with R^2 calculated using method proposed by Nagelkerke (1991). Co-efficient for individual predictors available from authors on request.

security issue	Participants (n=276) concerned about this issue (%)	χ^2	d.f.	p	R^2
shoulder surfing	34	8.48	12	0.75	0.05
skimming	29	11.23	12	0.51	0.07
personal theft/robbery	20	8.11	12	0.78	0.05
card or cash trap	18	10.53	12	0.57	0.07
other	19	20.3	12	0.06	0.13

Table 4: How does concern about ATM security influence your behaviour when using an ATM? (n = 236)

Security measure		Participants stating they take this measure (%)
ATM selection		
Only use ATM that is ...		28
	in branch/secure area	8
	in a busy area	8
	clean, new or 'safe'	7
	familiar to customer	5
Minimise ATM use		9
Avoid ATMs at weekends		1
ATM use		
Cover PIN		19
Check ATM before use		18
Look for suspicious people		8
'Be suspicious'		7
Look around or check area		6
Look over shoulder		3
Avoid interacting with other people		3
Other		7

Table 5: What factors do you consider when choosing an ATM to use? (n = 274)

Each model attempted to predict behaviour based on age, gender, previous victimisation and interview location – in no case were the results significant. Table shows logistic regression results, with R2 calculated using method proposed by Nagelkerke (1991).

security issue	Participants considering this factor	χ^2	d.f.	p	R^2
well-maintained ATM	73%	8.11	12	0.78	0.05
ATM in particular place	55%	10.53	12	0.57	0.07
ATM in busy area	52%	11.23	12	0.51	0.07
ATM in well-lit area	21%	8.48	12	0.75	0.05
particular brand of ATM	5%	20.3	12	0.06	0.13

Table 6: Which of the following security measures do you take when using an ATM? (n = 273)

Security measure	Participants stating they take this measure (%)
Covering ATM keypad when entering PIN	90
Checking ATM for suspicious devices	63
Checking that no one is standing close by	42
Checking over shoulder	40

Appendix A: survey questions

1. Are you conscious of security when using an ATM?
2. What security issues are you conscious of?
3. How does concern about ATM security influence your behaviour when using an ATM?
4. Have you been a victim of ATM crime?
5. Can you describe to me what happened when you were a victim of ATM crime?
6. Do you:
    a. cover your PIN?
    b. ensure no-one is in your personal space before using the ATM?
    c. request privacy when using the ATM?
7. What is the most important factor to you in deciding to use an ATM?
8. What is the most important factor to you when using an ATM?
9. Have you ever wanted to request privacy while using an ATM?